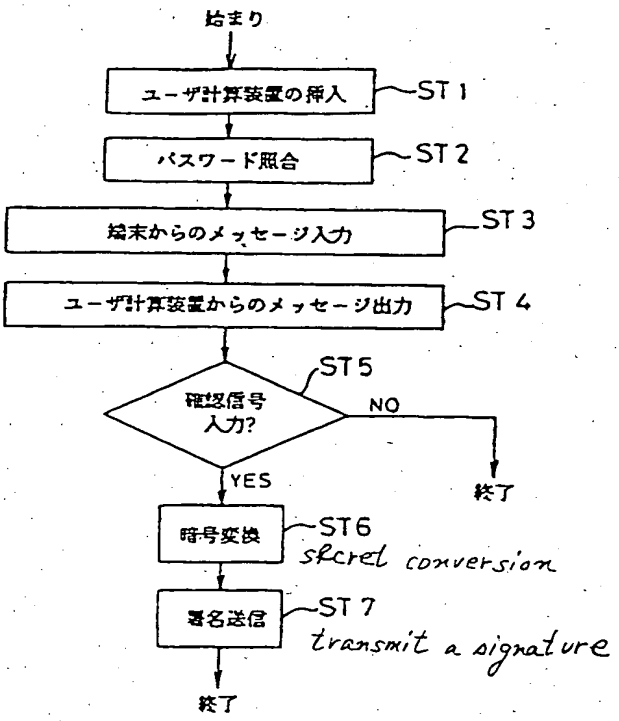
PAGE 9

1. **Title:** AN ELECTRONIC SIGNATURE CREATING APPARATUS
Laid-open Publication Number: 3-26126
Date of Publication: February 4, 1991
Applicant: TOSHIBA
Summary: A digital signature S is created in an IC card 3 (Fig.2) or 3' (Fig.3) from a message M and a secret key, which is stored in the IC card.

The related description is shown as: "The calculation portion 5 performs a secret conversion on a message M using a secret key stored in the storage portion 9 in the independent or dependent calculation method to create a signature S (see step ST6 of Fig.3). Then, the calculation portion 5 provides the signature S obtained by the secret conversion process and the message M as the target of the signature to the external terminal 1 through a transmitter 6 and an IC card reader/writer 2, and transmits them to another terminal via a communication network or stores them into the external terminal 1 (see step ST7 of Fig.3)."

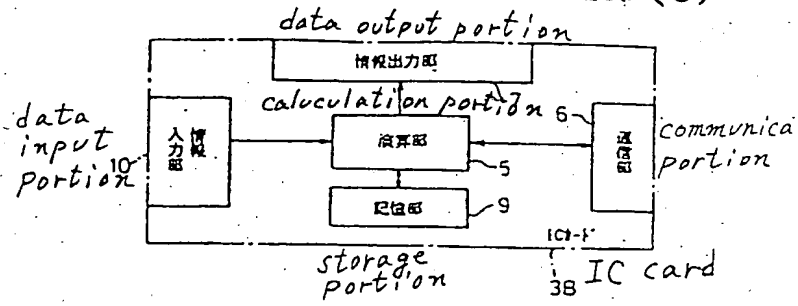
Further, in an IC card 3b of Fig.4, an information input portion 10 may be included, therefore, the contents of the message M can be inputted using the information input portion 10.

The English translation of terms used in Figs.3, 4 and 6 is attached hereinafter.

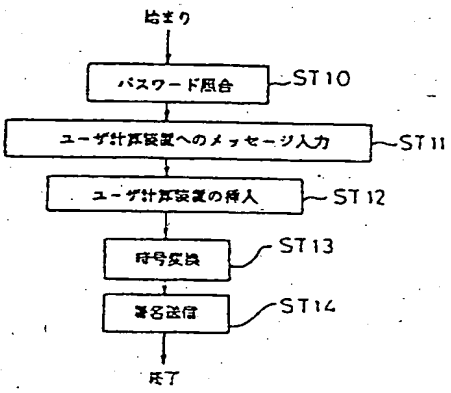


第 3 図

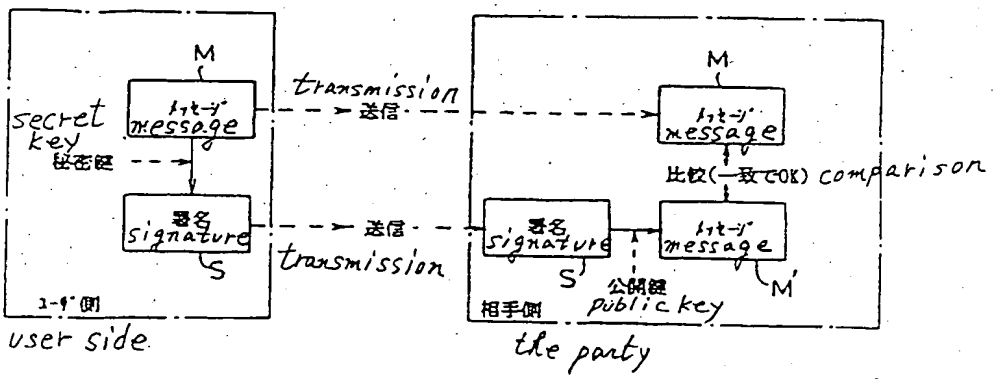
FIG. 3



第 4 図 Fig. 4



第 5 図



第 6 図

Fig. 6

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平3-26126

⑤Int.Cl.⁵	識別記号	庁内整理番号	⑬公開
H 04 L 9/32			
G 06 K 17/00	V	6711-5B	
G 09 C 1/00		7343-5B	
		6945-5K	H 04 L 9/00 A

平成3年(1991)2月4日

審査請求　未請求　請求項の数 2　(全6頁)

⑭発明の名称　電子署名作成装置

⑳特　願　平1-159767

㉒出　願　平1(1989)6月23日

⑦発明者　新保　淳　神奈川県川崎市幸区小向東芝町1　株式会社東芝総合研究所内

⑦発明者　川村　信一　神奈川県川崎市幸区小向東芝町1　株式会社東芝総合研究所内

⑦出願人　株式会社東芝　神奈川県川崎市幸区堀川町72番地

⑦代理人　弁理士　三好　秀和　外1名

明　細　書

1．発明の名称

電子署名作成装置

2．特許請求の範囲

(1)ネットワークに接続される端末と、この端末に接続されるユーザ側固有計算装置とを備えた電子署名作成装置において、

前記ユーザ固有計算装置側に、

秘密鍵を格納する格納部と、

前記端末側から供給されるメッセージの内容をユーザ側に知らせる出力部と、

ユーザによって署名の許可、不許可の指示が入力される署名可否入力部と、

この署名可否入力部から署名許可指示が入力されたとき前記格納部に格納されている秘密鍵を用いて前記メッセージに対する署名を作成して前記端末側に送る演算部と、

を設けたことを特徴とする電子署名作成装置。

(2)前記ユーザ固有計算装置側に、メッセージを入力するためのメッセージ入力部を有し、このメッセージ入力部から入力されたメッセージを署名対象とする請求項1記載の電子署名作成装置。

3．発明の詳細な説明

〔発明の目的〕

(産業上の利用分野)

本発明は公開鍵暗号の署名機能を利用する情報通信システムに適用され、署名作成を安全に実行する電子署名作成装置に関する。

(従来の技術)

情報通信システムにおいては、受信したメッセージの作成者が誰なのか、メッセージが送信者の作成したままで改ざんされていないのか、通信相手は相手本人に間違いないかなどを認証することが重要な要件となっている。

このような情報通信システムにおける認証機能を実現する方法として、暗号技術、特に公開鍵暗号を利用することが考えられている。

RSA(Rivest-Shamir-Adleman)暗号に代表される公開鍵暗号は、公開鍵と、秘密鍵とを使い分けることが特徴である。

この場合、秘密鍵は各ユーザ毎に異なり、各ユーザが秘密に保持し、一方公開鍵（これもユーザ毎に異なる）はデータベースのような形で公開され、改ざんされないように安全に管理される。

そして、このような公開鍵暗号を利用した認証法はデジタル署名という方法に集約される。

このデジタル署名では、第６図に示す如くメッセージＭにユーザが秘密鍵で暗号変換を施して署名Ｓを作成し、これらを相手側に送信する。そして、この相手側で公開鍵を使用して署名Ｓを逆変換してメッセージＭ' を作成し、このメッセージＭ' とユーザ側から送信されたメッセージＭとが一致しているときユーザ側から送られたメッセージＭがユーザによって作成されたものであると判定する。

このデジタル署名の機能により、将来的には情報通信システムにより電子取引や電子資金移動などのサービスが可能になるものと期待される。

しかしこのようなサービスが実現された場合、ユーザのデジタル署名は今日の約束手形等の証明と同じ役割を担うため、署名の偽造、不正取得（だまし取り）などの行為は厳に防止されなければならない。

このため、ユーザの秘密鍵は、ＩＣカードのようなアクセス制御能力のある記憶媒体に格納されて発行されることが予想される。

しかし現在のところ、ＩＣカードの計算能力はＲＳＡ暗号などの秘密変換（署名変換）を実現するには不十分であるため、外部端末であるワークステーションやパーソナルコンピュータの計算能力を借りることが実際的である。

ところが、秘密鍵の情報を外部端末に漏らすのは好ましくない。

このように、秘密鍵の情報を外部端末に漏らさず、外部端末の計算能力を借りる方法として、最近、依頼計算なる方法が提案されている（電子情報通信学会技術研究報告ＩＳＥＣ８８－９等）。

この方法によれば、ＩＣカードから外部に秘密鍵が漏れることを防止することができ、ＩＣカード側で単独で変換処理を実行するよりも高速に秘密変換を実行することができる。

また、将来的には、秘密変換を高速で実現できる装置がＩＣカード内に装備され、ＩＣカード単独で秘密変換を高速で実現できるようになるとも考えられる。

しかしながら、このように個人秘密鍵をＩＣカード外部に漏らさずに高速に秘密変換を実行できると仮定しても次に述べるような端末側の不正行為が考えられる。

一般の署名作成手順に対応づけてこの手順を説明する。

まず、ユーザが端末のカードリーダに自分のＩＣカードを挿入し、端末のキーボードから署名作成対象となるメッセージＭを入力したり、電子的なファイルとして署名作成対象となるメッセージＭを端末のフロッピーディスクドライバから入力したりしたとき、端末側が前記メッセージＭと異なるメッセージＭ' をＩＣカードに送ると、ＩＣカードはメッセージＭ' に対する署名Ｓ' を作成する。

この場合、ユーザ側が署名したいメッセージＭと異なるメッセージＭ' に対して署名したことになる。

即ち、ユーザとＩＣカードとのインタフェースとして、端末が介在しているため、端末がユーザの意図しないメッセージＭ' に対する署名をだまし取ることができる。

（発明が解決しようとする課題）

以上述べてきたように、従来のＩＣカードに代表されるユーザ固有計算装置と端末を用いて署名作成を行なう場合には、端末による不正な署名の取得が可能であるため、これを完全に防止することができるシステムの開発が強く望まれていた。

本発明は上記の事情に鑑み、端末による不正行為を完全に防止することができ、これによって署名の安全性を大幅に高めることができる電子署名作成装置を提供することを目的としている。

〔発明の構成〕

（課題を解決するための手段）

上記の目的を達成するために本発明による電

子署名作成装置は、ネットワークに接続される端末と、この端末に接続されるユーザ側固有計算装置とを備えた電子署名作成装置において、前記ユーザ固有計算装置側に、秘密鍵を格納する格納部と、前記端末側から供給されるメッセージの内容をユーザ側に知らせる出力部と、ユーザによって署名の許可、不許可の指示が入力される署名可否入力部と、この署名可否入力部から署名許可指示が入力されたとき前記格納部に格納されている秘密鍵を用いて前記メッセージに対する署名を作成して前記端末側に送る演算部とを設けたことを特徴としている。

（作用）

上記の構成において、端末側からユーザ固有計算装置側にメッセージが出力されたとき、出力部によってこのメッセージの内容をユーザ側に知らせ、これに対応してユーザ側が署名可否入力部から署名許可指示を入力したとき演算部によって格納部に格納されている秘密鍵が用いられて前記メッセージに対する署名が作成されこの署名が前記端末側に送られる。

（実施例）

第１図は本発明による電子署名作成装置の一実施例を示すブロック図である。

この図に示す電子署名作成装置は、情報通信ネットワークに接続されたパーソナルコンピュータ等によって構成される外部端末１と、この外部端末１に接続されるＩＣカードリーダライタ２と、各ユーザ固有の計算装置として使用されるＩＣカード３とを備えており、ＩＣカード３がＩＣカードリーダライタ２に挿入されて、ユーザによる署名作成が行われるとき、署名対象となるメッセージＭをＩＣカード３上に表示させてユーザにメッセージＭの内容を確認させて署名動作を行なわせる。

この場合、ＩＣカード３は第２図に示す如くユーザの秘密鍵やユーザのパスワード等が格納されている記憶部９と、この記憶部９に格納されている前記秘密鍵を用いて単独あるいは依頼計算という手法による外部端末１の計算能力を一部利用して暗号変換処理を高速で実行したり、署名対象となるメッセージＭを表示させたりする演算部５と、ＩＣカード３がＩＣカードリードライタ２に差し込まれたとき、前記演算部５と前記ＩＣカードリードライタ２とを電気的に接続する通信部６と、前記演算部５から出力されるメッセージＭをユーザ等に表示する情報出力部７と、この情報出力部７に表示されたメッセージＭの内容に応じてユーザが署名するとき操作される署名作成確認信号入力部８とを備えている。

次に、第３図に示すフローチャートを参照しながらこの実施例の動作を説明する。

まず、署名動作に先立って、ユーザはＩＣカード３をＩＣカードリーダライタ３に挿入する（ステップＳＴ１）。

この後、ユーザによって外部端末１のキーボードが操作されてパスワードが入力されると、外部端末１はＩＣカードリーダライタ２、ＩＣカード３の通信部６を順次介して前記パスワードを演算部５に供給し、このパスワードと、記憶部９に格納されているパスワードとが一致しているかどうかをチェックさせる（ステップＳＴ２）。

そして、これらが一致していなければ、演算部５はパスワードエラーメッセージを作成してこれを外部端末１側に送り、この外部端末１のＣＲＴ上に“パスワードエラー”等のメッセージを表示させる。

この後、所定回数以内で、正しいパスワードが入力されれば、外部端末１はメッセージ受付可能状態になる。

ここで、この外部端末１のキーボード等を操作したり、外部端末１のフロッピーディスク装置にメッセージＭが格納されているフロッピーディスクをセットしたり、情報通信ネットワークを介して電子メールのような形式で他端末から送られたメッセージＭを選択したりして、署名対象となるメッセージＭの入力動作を行なえば、外部端末１はＩＣカードリーダライタ２、ＩＣカード３の通信部６を順次介して署名対象となるメッセージＭを演算部５に供給する（ステップＳＴ３）。

そして、演算部５はこのメッセージＭを情報出力部７に供給してユーザにメッセージＭの内容を提示する（ステップＳＴ４）。

ここで、この情報出力部７に表示されたメッセージＭの内容を見たユーザがこのメッセージＭに署名をしても良いと判断して署名作成確認信号入力部８の確認キーを押せば（ステップＳＴ５）、演算部５はこれを検知して記憶部９に格納されている秘密鍵を使用して単独計算手法あるいは依頼計算手法でメッセージＭに対する秘密変換を行ない署名Ｓを作成する（ステップＳＴ６）。

この後、演算部５はこの秘密変換処理によって得られた署名Ｓと、署名の対象となったメッセージＭとを通信部６、ＩＣカードリーダライタ２を順次介して外部端末１に供給し、これを情報通信ネットワークを介して他端末に伝送させたり、外部端末１に格納させたりする（ステップＳＴ７）。

また、上述したメッセージＭのチェック処理において（ステップＳＴ５）、所定時間内にユーザが署名作成確認信号入力部８の確認キーを押さない場合や、署名作成不許可キーを押した場合には、演算部５は秘密変換処理を中止して処理を終了する。

このようにこの実施例においては、ＩＣカード３側に情報出力部７を設け、署名の対象となるメッセージＭを情報出力部７に表示させてユーザにメッセージＭの内容を確認させるようにしているので、外部端末１や他端末による不正行為を完全に防止することができ、これによって署名の安全性を大幅に高めることができる。

また上述した実施例においては、ＩＣカード３がＩＣカードリーダライタ２内に挿入されている状態で、情報出力部７がＩＣカードリーダライタ２から外に突出している場合を例にとって説明したが、ＩＣカード３がＩＣカードリーダライタ２内に挿入されている状態で、情報出力部７がＩＣカードリーダライタ２内にあり、外部から情報出力部７が直接見えない場合には、メッセージＭを確認するとき、ＩＣカードリーダライタ２からＩＣカード３を取り出し、この後署名作成確認信号入力部８を操作して署名作成の許可、不許可を入力した後、ＩＣカード３をＩＣカードリーダライタ２に挿入して処理を続行させるようにしても良い。

また上述した実施例においては、署名許可キー、署名不許可キーを設けたＩＣカード３を使用するようにしているが、このようなＩＣカード３に代えて、第４図に示すようなＩＣカード３ｂを使用するようにしても良い。なおこの図において、第２図の各部と対応する部分には同じ符号が付してある。

この図に示すＩＣカード３ｂが第２図に示すものとことなる点は、署名作成確認信号入力部８に代えてキーボード等を有する情報入力部１０を設け、この情報入力部１０のキーボードを操作することによって署名許可、署名不許可の指令やメッセージＭの内容を入力し得るようにしたことである。

そしてこの場合、第５図のフローチャートで示す手順で署名作成動作が行われる。

まず、署名動作に先立って、ユーザはＩＣカード３ｂをＩＣカードリーダライタ２に挿入する（ステップＳＴ１０）。

この後、ユーザによって外部端末１のキーボードが操作されてパスワードが入力されると、外部端末１はＩＣカードリーダライタ２、ＩＣカード３の通信部６を順次介して前記パスワードを演算部５に供給しこのパスワードと、記憶部９に格納されているパスワードとが一致しているかどうかをチェックさせる（ステップＳＴ１１）。

そして、これらが一致していなければ、演算部５はパスワードエラーメッセージを作成してこれを外部端末１側に送り、この外部端末１のＣＲＴ上に"パスワードエラー"等のメッセージを表示させる。

この後、所定回数以内で、正しいパスワードが入力されれば、外部端末１はメッセージ受付可能状態になる。

ここで、ユーザがＩＣカードリーダライタ２からＩＣカード３ｂを取り出して情報入力部１０に

設けられたキーボードを操作し署名対象となるメッセージMを入力すれば、演算部5はこれを取り込むとともにこれを情報出力部7に供給してユーザにメッセージMの内容をユーザに提示する。

ここで、この情報出力部7に表示されたメッセージの内容を見たユーザがこのメッセージMに署名をしても良いと判断して情報入力部10のキーボードを操作して署名許可指令を入力すれば、演算部5はこれを検知して内部メモリ内の署名許可フラグをセットする（ステップST11）。

この後、ユーザがICカード3bをICカードリーダライタ2に挿入すれば、演算部5は内部メモリ内の署名許可フラグがセットされているかどうかをチェックし、これがセットされていれば、記憶部9に格納されている秘密鍵を使用して単独計算手法あるいは依頼計算手法でメッセージMに対する秘密変換を行ない署名Sを作成する（ステップST13）。

この後、演算部5はこの秘密変換処理によって得られた署名Sと、署名の対象となったメッセージMとを通信部6、ICカードリーダライタ2を順次介して外部端末1に供給し、これを情報通信ネットワークを介して他端末に伝送させたり、外部端末1に格納させたりする（ステップST14）。

このようにこの実施例においては、ICカード3b上にキーボード等を有する情報入力部10を設け、この情報入力部10のキーボードを操作することによって署名許可、署名不許可の指令やメッセージMの内容を入力し得るようにしたので、外部端末1や他の端末による不正行為を完全に防止することができる。

〔発明の効果〕

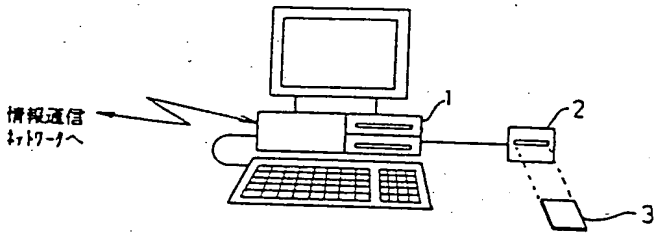
以上説明したように本発明によれば、端末による不正行為を完全に防止することができ、これによって署名の安全性を大幅に高めることができる。

4．図面の簡単な説明

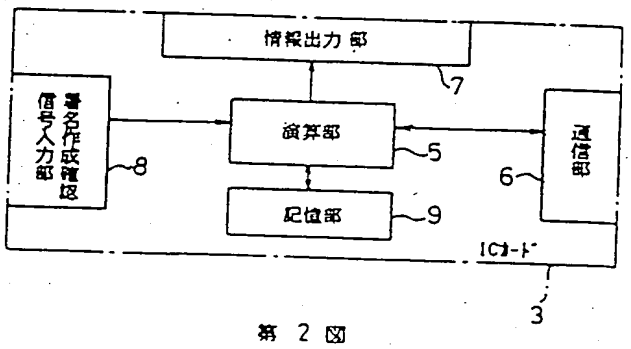
第1図は本発明による電子署名作成装置の一実施例を示すブロック図、第2図は第1図に示すICカードの詳細なブロック図、第3図は同実施例の動作例を示すフローチャート、第4図は本発明による電子署名作成装置の他の実施例で用いられるICカードの詳細なブロック図、第5図は第4図に示すICカードを用いたときの動作例を示すフローチャート、第6図はデジタル署名を説明するための模式図である。

1…端末（外部端末）
2…ICカードリーダライタ
3…ユーザ側固有計算装置（ICカード）
5…演算部
7…出力部（情報出力部）
8…署名可否入力部（署名作成確認信号入力部）
9…格納部（記憶部）

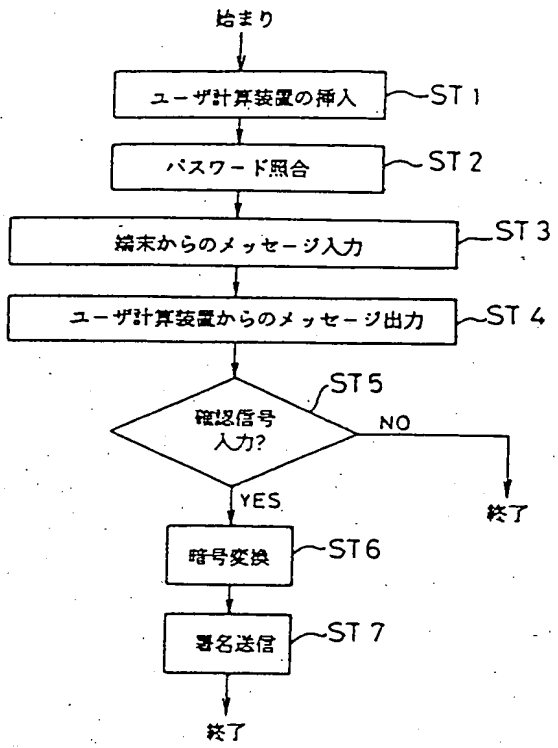
代理人弁理士 三好秀和



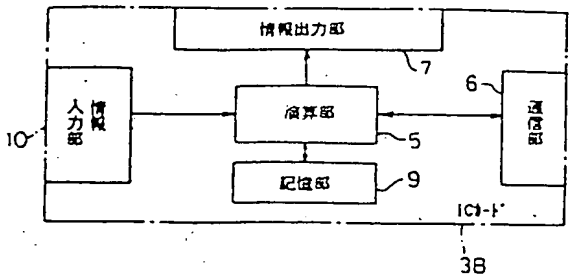
第1図



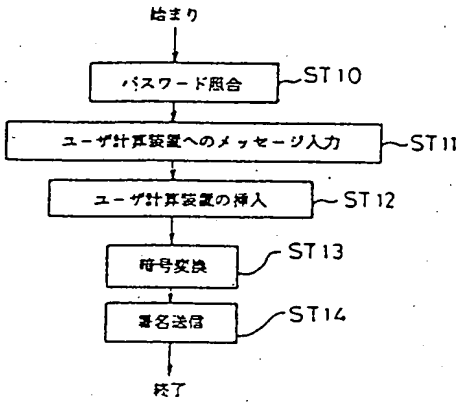
第2図



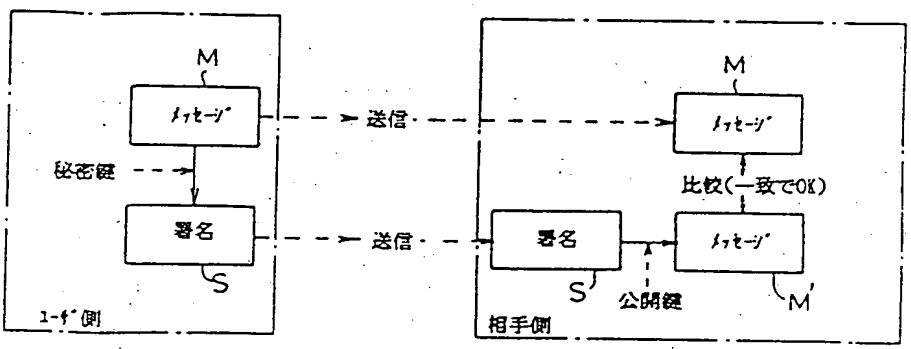
第 3 図



第 4 図



第 5 図



第 6 図